Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 12, Issue. 4, April 2023, pg.1 – 16

Multiple 3D Chaotic Keys to Protect Digital Images

Prof. Ziad Alqadi; Dr. Rushdi Abu Zneit
Albalqa Applied University, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i04.001

Abstract: A simple, multipurpose, efficient, sensitive and highly qualities method of image cryptography will be introduced in this research paper. The method will be easily used to encrypt-decrypt any type of image with any size (gray and color images). The proposed method will secure the image by providing a high degree of image protection based on using a complex private key, which contains eight values, each of the has a double data type. The private key will provide the required key space to resist any hacking attack. The private key components will be used to calculate the size of the generated 3D chaotic logistic key. The private key will also be used to run two chaotic logistic map models to get two different chaotic keys base on the chaotic parameters values included in the private key. Two rounds of XORing operations will be used to generate the encrypted-decrypted image. The generated outputs of the proposed method will be sensitive to the selected value of the private key. The proposed method will be very flexible, changing the source image or/and changing the private key will not require any changes in the method algorithm. The proposed method will be tested and implemented using various image, the obtained results will be discussed to prove the features provided by the method: quality, sensitivity, security and efficiency.
Keywords: Cryptography, quality, sensitivity, performance, CLK, CLMM, MSE, PSNR, NPCR.

Introduction

Digital images [11-18], regardless of their type (gray or color), are considered one of the most important types of data circulated through various means of communication due to their use in many important vital applications. The wide spread of digital images is due to many reasons, the most important of which are [19-25]:

- It can be used in countless computer applications, for example, but not limited to: medical, educational, security and banking applications.
- Ease of obtaining and keeping it due to the multiplicity of different sources that it provides and at no cost.
- Availability of various equipments which can easily generate any digital image.

- The ease of digital image processing, the gray image is represented by a 2D matrix (see figure 1), while the color image is represented by a 3D matrix (see figure 2), so image processing is transformed into a matrix processing process [26-35].
- The large size of the digital image, which makes it a large data store that can be used for a variety of purposes.

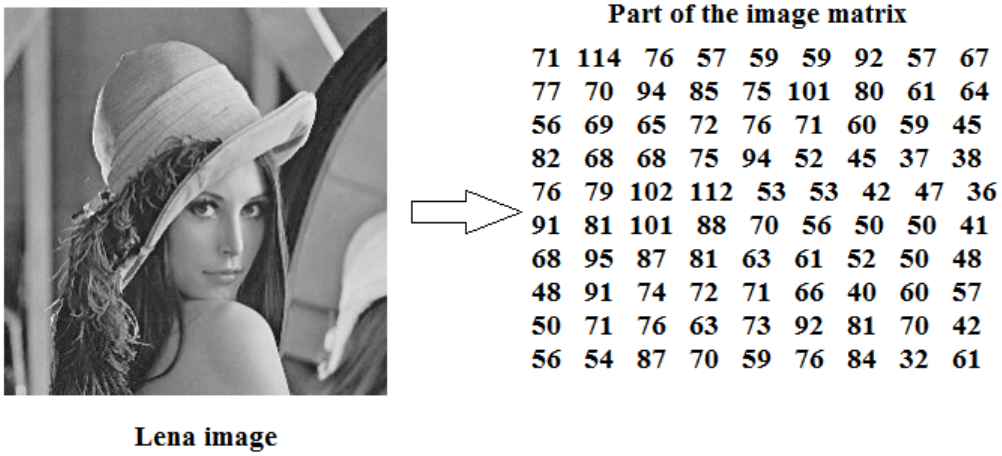

Figure 1: Gray image sample

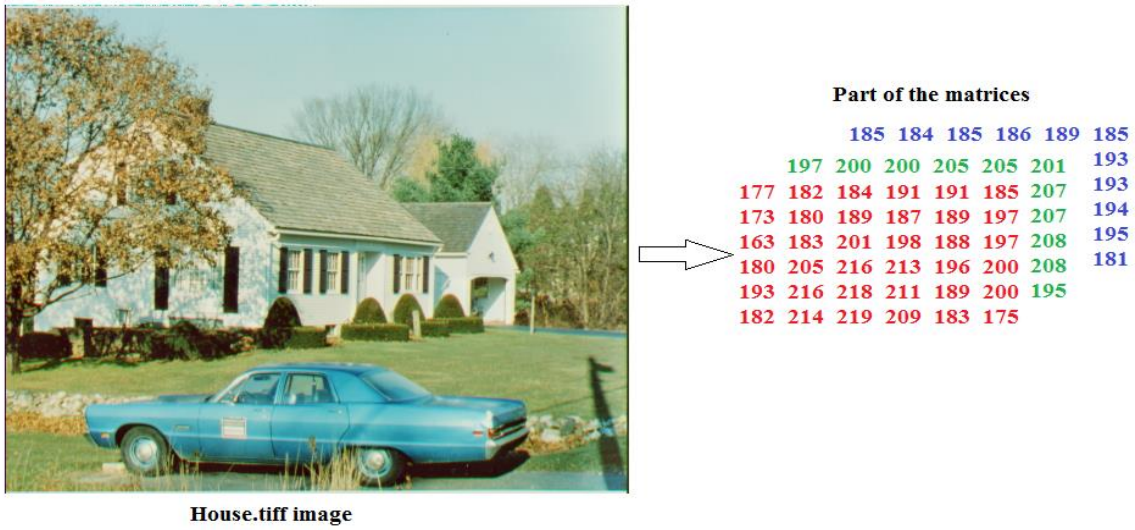

Figure 2: Color image sample

Digital image require protection from for the following reasons [36-42]:

- It may be secret.
- It may of special nature.
- It may contain secret information and it is used as a stego image.

And due to these reasons and due to the importance of digital images, the number of people lurking in them has increased, which requires us to provide the necessary protection for them, especially if the communication environment is not safe. The protection must prevent the image from being hacked [43-50].
One of the most popular methods used in image protection is image cryptography, which means encrypting the image before sending and decrypting the image after receiving. Image encryption system as shown in figure 3 contains: original image, encrypted (cipher) image, encryption function and one or more private keys. The decryption systems contains: encrypted image, decrypted image, decryption function and the same PKs used in the encryption system [51-60].

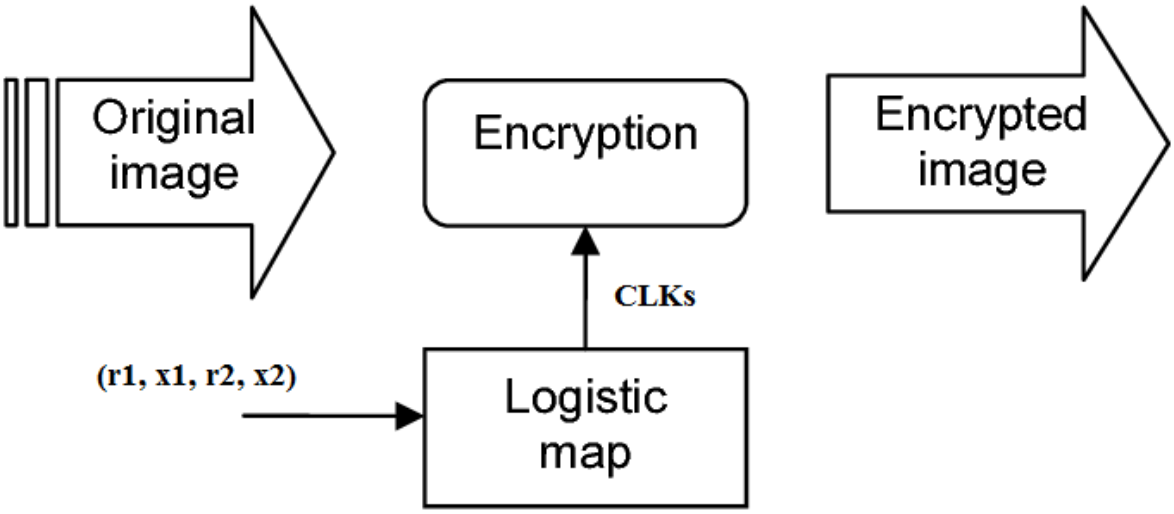

Figure 3: Encryption system

The encryption function uses the PKs to manipulate the original image to produce a damaged scrambled encrypted image, while the decryption function uses the same PKs to manipulate the encrypted image to produce a decrypted image, which is identical to the source original image [61-65].
Chaotic logistic map can be easily used to generate the required secret keys needed in the encryption and decryption functions [66-73]. The chaotic parameters r and x are used to run the chaotic logistic map model (CLMM), to generate a chaotic logistic key (CLK) [1-9], this key can be easily converted to integer decimal to match the values of the digital image. Chaotic parameters can are used to generate1D matrix CLK [1-4], also these parameters can be used to generate a 3D CLK by setting the size to a selected values, the following sequence of matlab operations can be used to generate a 3D CLK:


```
%Chaotic parameters:
r1=3.77;x1=0.1;
%Three loops (R1 and C1 are the sizes)
for i=1:R1
   for j=1:C1
      for k=1:3
       x1=r1*x1*(1-x1); %Chaotic logistic equation
      CLK1(i,j,k)=x1;
       end
   end
end
%Converting CLK to decimal integers
key1=uint8(255*CLK1);
```

The CLK generation process require a time and this time will grow up when the key size increases, so it is recommended to generate a small in size chaotic key [61-67], then the obtained key can be easily resized to match the size of the image [55-60].

Many authors [1-10] used the idea of chaotic logistic theory to build various schemas of image encryption-decryption; these methods share some good features such as quality of cryptography, security by providing acceptable key space. The introduced methods provided throughputs, which some times were low and they were varied from 19.7470 K bytes per second [4] to 231.0469 K bytes per second [9].

The aim of this paper research is to introduce a method of image cryptography to achieve the following:

- Multiple purposes to be used to encrypt-decrypt any image with any size and type.
- Simplicity and flexibility, changing the image or/and changing the PK must not affect the method algorithm; also simplify the encryption and decryption functions by reducing the number of used operations to apply encryption and decryption processes.
- High performance, decreasing the encryption-decryption time and increasing the throughput of digital image cryptography [65-73].
- High quality, the encrypted image must be totally damaged and scrambled, while the decrypted image must be identical to the source image [60-64].
- High security, increasing the key space and making the produced outputs very sensitive to the selected values of the PK.

The Proposed Method

The proposed method uses a complicated PK, which contains the value of 8 double types values as shown in figure 4. The parameters P1, P2, P3and P4 are a partition fractions used to select the row sizes and column sizes of the two chaotic logistic keys (CLK) to be generated, while r and x are the chaotic logistic parameters needed to execute the chaotic equation and run the chaotic logistic map model (KLMM).

Parameters to set the size of the 3D CKs			
Row fraction for CK 1	Column fraction for CK 1	Row fraction for CK 2	Column fraction for CK 2
P1	P2	P3	P4
Chaotic logistic Parameters			
r1	x1	r2	x2
Example of PK			
0.1	0.017	0.056	0.21
3.77	0.1	3.92	0.23

Figure 4: PK structure

The generated CLKs must be converted to decimal integers to form the secret keys required to apply XORing operation, the generated secret is to be resized to match the image size. The generated secret key is very sensitive to the selected values of the PK components, any minor changes in one or more values will generate a new key as shown in the examples illustrated in figures 5, 6, and 7 (image size in the examples was 20x35)

PK1:
n1=20;n2=35;n3=3;
p1=0.19;p2=0.17;
p3=0.087;p4=0.076;
r1=3.77;x1=0.1;
r2=3.66;x2=0.12;

```
key1(:,:,1) =                    key1(:,:,2) =                    key1(:,:,3) =

   87  240  228  110  185          216   52   92  236  192          126  157  221   66  179
  202   98  222   72  207          159  227  107  194  147          226   93  234  175  235
   70  197  124  157  223          191  168  240  227  104          181  216   53   94  232
```

Figure 5: Generated key 1 using PK1 (example)

PK2:
n1=20;n2=35;n3=3;
p1=0.19;p2=0.17;
p3=0.087;p4=0.076;
r1=3.92;x1=0.1;
r2=3.66;x2=0.12;

```
key1(:,:,1) =                 key1(:,:,2) =                 key1(:,:,3) =

   90  233  130   73  232       228   80  250  203   81       94  216   20  161  217
  128   71  225   53   89       250  201  103  164  227       20  168  241  230   96
  235  163  225   54  100        72  230  103  167  238      203   88  240  226   61
```

Figure 6: Generated key 1 using PK2 (r1 was changed: example)

PK3:

n1=20;n2=35;n3=1;
p1=0.19;p2=0.17;
p3=0.087;p4=0.076;
r1=3.77;x1=0.25;
r2=3.66;x2=0.12;

```
key1 =

   187   195   180   207   153
   240    57   173   218   123
   250    21    75   207   153
```

Figure 7: Generated key 1 using PK3 (n3 and r1 were changed: example)

The proposed method encryption phase can be implemented applying the following steps:

Step 1:

Image preparation: Get the image; retrieve the image size, this step can be implemented applying the following mat lab sequence of operations:

```
a=imread('C:\Users\win 7\Desktop\st_images\4.2.07.tiff');
[n1 n2 n3]=size(a);s=n1*n2*n3;
```

Step 2:

Key size calculation: get the PK, use P1, P2, P3, and P4 to calculate the sizes of the two CLKs, this step can be implemented applying the following mat lab sequence of operations:

```
p1=0.9;p2=0.09;
p3=0.087;p4=0.076;
r1=3.77;x1=0.1;
r2=3.66;x2=0.12;
R1=fix(p1*n1);C1=fix(p2*n2);
R2=fix(p3*n1);C2=fix(p4*n2);
```


Step 3:

Secret keys generation: Use the chaotic logistic parameters values included in the PK to run two CLMM to get two CLKs, convert them to integers and then resize each of them to the image size, this step can be implemented applying the following mat lab sequence of operations:

```
for i=1:R1
   for j=1:C1
      for k=1:n3
       x1=r1*x1*(1-x1);
      CLK1(i,j,k)=x1;
       end
   end
end
key1=uint8(255*CLK1);
key11=imresize(key1,[n1 n2]);
for i=1:R2
   for j=1:C2
      for k=1:n3
       x2=r2*x2*(1-x2);
      CLK2(i,j,k)=x2;
       end
   end
end
key2=uint8(255*CLK2);
key22=imresize(key2,[n1 n2]);
```

Step 4:

Encryption: XOR the image with the first key, XOR the results with the second key to get the encrypted image, this step can be implemented applying the following mat lab sequence of operations:

```
e1=bitxor(a,key11);
e=bitxor(e1,key22);
```

The decryption phase can be implemented applying the same steps as for encryption but using the encrypted image as an input image.

Implementation and Experimental Results

To demonstrate the proposed method, the method was applied using some image files taken from the http:// sipi.usc.edu/database/ that is also known as the USC-SIPI Image Database to analyze the utility and the do-ability of our proposed gray and RGB images cryptography scheme. All the related experiments and simulations have been performed in MATLAB environment.

For image cryptography we have selected the color image house.tiff with 512x512 sizes. The original house image shown in the Figure 8(a) was encrypted using the proposed method, figure 8(b) shows the encrypted image, while figure 8(c) shows the decrypted image. The encrypted image was completely scrambled and damaged without

leaving any clue to reveal the original image information. The decryption result indicates that the proposed method effectively works and perfectly recovers the original image without losing any piece of information from the original image.

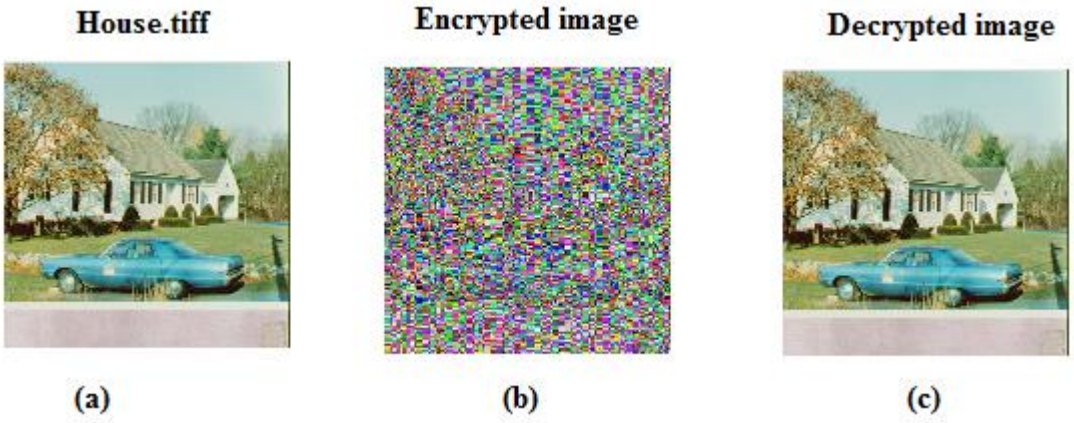

Figure 8: House.tiff cryptography results

A gray images were also implemented using the proposed method, the obtained encrypted images were totally damaged, while the decrypted image were always identical to the source images, figure 9 shows a sample outputs results of the proposed method implementations:

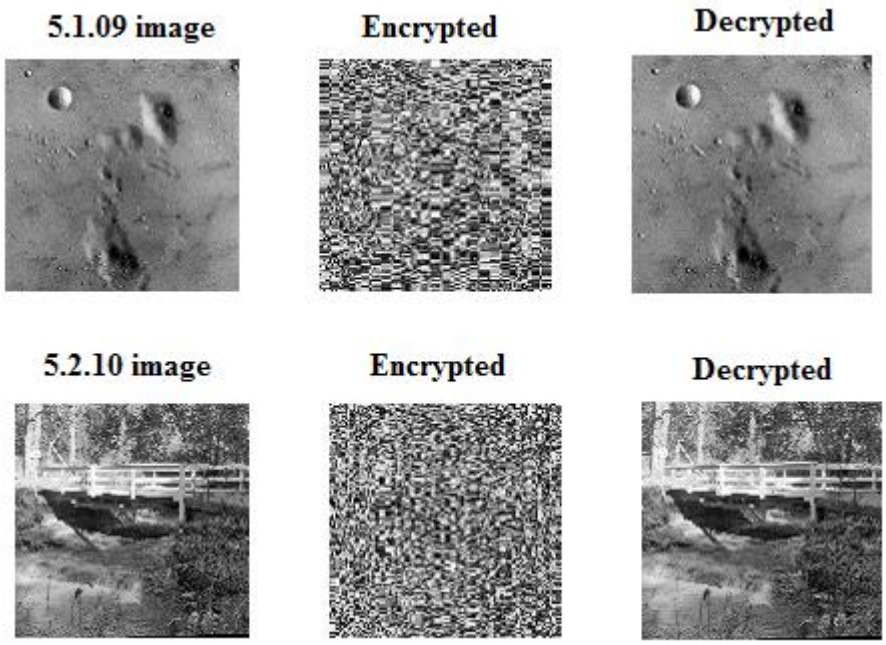

Figure 9: Gray images samples

The quality of image cryptography [60-60] can be measured by the calculated mean square error (MSE) between two images, and the peak signal to noise ratio (PSNR) between two images. In the encryption phase the value of MSE must be high, while the value of PSNR must be low. In the decryption phase the value MSE must be zero, while the value of PSNR must be infinite [11-17]. To prove that the proposed method satisfies the quality

requirements, some image were taken and the MSE and PSNR values were calculated, table 1 shows the obtained results for the encryption phase, for the decryption phase MSE was always zero and PSNR was always infinite[18-25]:

Table 1: Encryption quality results

Image	Size	MSE	PSNR
House	512x512x3	7857.3	21.1333
2.2.01	1024x1024x3	8023.8	20.9236
2.2.21	1024x1024x3	7665.0	21.3811
4.2.07	512x512x3	8529.8	20.3120
5.1.09	256x256	5980.9	23.8620
5.2.10	512x512	7624.9	21.4335
Remarks		High	Low
		Satisfy the quality requirements	

The sensitivity of the proposed method was tested. The Encryption and decryption phases must use the same private key (PK), any minor changes in the PK in the decryption phase will be considered as a hacking attempt by producing a damaged decrypted image. To show this an image was taken and encrypted using PK1 (from the list shown in figure 10), the encrypted image was decrypted by each of the listed PKs, figure 11 shows the obtained results:

PK1:
p1=0.01; p2=0.09; p3=0.087; p4=0.076; r1=3.77; x1=0.1; r2=3.66; x2=0.12;

PK2:

p1=0.03; p2=0.09; p3=0.087; p4=0.076; r1=3.77; x1=0.1; r2=3.66; x2=0.12;

PK3:

p1=0.01; p2=0.19; p3=0.087; p4=0.076; r1=3.77; x1=0.1; r2=3.66; x2=0.12;

PK4:

p1=0.01; p2=0.09; p3=0.187; p4=0.076; r1=3.77; x1=0.1; r2=3.66; x2=0.12;

PK5:

p1=0.01; p2=0.09; p3=0.087; p4=0.276; r1=3.77; x1=0.1; r2=3.66; x2=0.12;

PK6:

p1=0.01; p2=0.09; p3=0.087; p4=0.076; r1=3.97; x1=0.1; r2=3.66; x2=0.12;

PK7:

p1=0.01; p2=0.09; p3=0.087; p4=0.076; r1=3.77; x1=0.15; r2=3.66; x2=0.12;

PK8:

p1=0.01; p2=0.09; p3=0.087; p4=0.076; r1=3.77; x1=0.1; r2=3.76; x2=0.18;

Figure 10: Used PKs

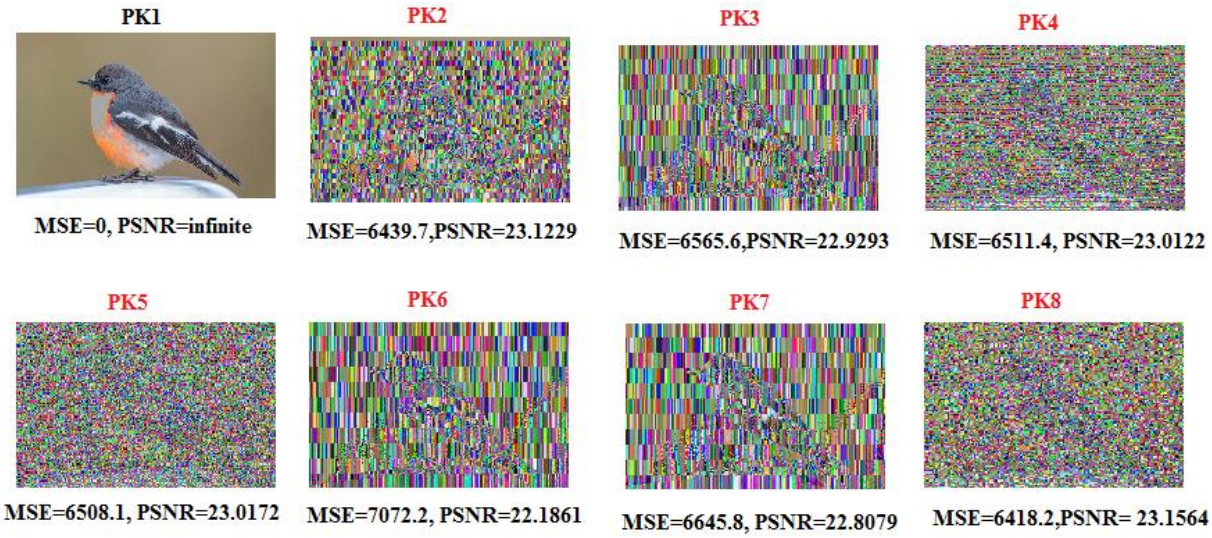

Figure 11: Decrypted images using various PKs in the decryption phase

The obtained images (shown in figure 11) show that the proposed method is very sensitive to the selected values of the PK, any changes in one of them or more will lead to produce a damaged decrypted image.

The proposed method algorithm should be able to resist a differential attack. It is one of the most efficiently and commonly used methods by the hackers to come across significant information between the plain source image and the cipher encrypted image. Indicators like number of changes pixel ratio (NPCR) is used to quantify the ability of an encryption algorithm to test the effectiveness of being sensitive when the plain image is changed or modified during transmission or any stage by different attacks. NPCR determines the change rate in number of pixels between two images C1 and C2. An effective cryptosystem yields close to 100 percent which indicates maximum resistance to differential attack. The value of NPCR can be calculated using equation (1):

$$NPCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} Z(a,b)}{H*W} \quad \textbf{(1)}$$

Where:

$$Z(a,b) = 1 \text{ if } C1 \neq C2 \text{ and } = 0$$

$$\text{if } C1 = C2$$

and H is the row size, W is the column size

A comparison is carried out among different schemes [1-4] and the values are furnished in Table 2. The NPCR value for the Lena image is obtained as 99.7305and the result is relatively satisfactory with those of other methods.

Table 2: NPCR measure for different methods

Method	NPCR
Reference [1]	99.60
Reference [2]	99.6506
Reference [3]	99
Reference [4]	99.66
Proposed	99.7305

The proposed method provides a huge key space capable to resist hacking attacks, the PK contains 8 components, each of which has a double data type (64 bits representation), so the key space can be calculated as shown in equation 2:

$$\text{Key space} = 2^{8x64} = 2^{512} \quad (2)$$

This key space is better than other introduced methods key spaces as shown in table 3.

Table 3: Methods key space comparisons

Method	Key space
Reference [5]	2^{128}
Reference [6]	2^{149}
Reference [7]	2^{209}
Reference [8]	2^{256}
Reference [9]	2^{398}
Proposed	2^{512}

The speed of the proposed method was tested, some images were selected and treated using the proposed method, the encryption times and the throughputs were calculated, table 4 shows the obtained results:

Table 4: Proposed method speed results

Image	Size in bytes	Encryption time (second)	Throughput (K bytes per second)
Lena	65536	0.0480	1333.3
House	786432	0.0790	9721.5
2.2.01	3145728	0.4890	6282.2
2.2.21	3145728	0.4890	6282.2
4.2.07	786432	0.0790	9721.5
5.1.09	65536	0.0480	1333.3
5.2.10	262144	0.0550	4654.5
Average	1179648	0.1839	5618.4

From table 4 we can see that the proposed method provides a good throughput of average equal 5618.4 K bytes per second, for comparison purposed the image Lena was encrypted using the introduced methods in [4] and [9]. Table 5 shows the results of comparisons:

Table 5: Encryption time comparisons

Method	Encryption time (second)	Throughput (K bytes per second)	Speed up of the proposed method
Reference [4]	3.241	19.7470	67.5208
Reference [9]	0.277	231.0469	5.7708
Proposed	0.0480	1333.3	1.0000
	Speed up of the proposed method equal time of other method divided by proposed time		

From table 5 we can see that the proposed method enhance the performance of image cryptography by decreasing the encryption time.

Conclusion

An efficient method of image cryptography was introduced, tested and implemented. The proposed method provided a good performance by decreasing the encryption-decryption time and increasing the throughput of image cryptography, the method provided a significant speed up comparing with other methods of image cryptography. The proposed method used a private key with complicated structure, this key was used to set the length of the 3D chaotic logistic keys and it was used to generate them. To minimize and save the key generation time the key sizes were small and they were resized to the size of the image to be encrypted-decrypted. The proposed method provided a good level of security, this level is better than theses for other existing method, the key space and

sensitivity analysis showed that the proposed method can resist hacking attacks. The proposed method used simplified encryption-decryption functions; these functions used a two round XORing to encrypt-decrypt the image. The proposed method was flexible, it used gray and color images, changing the image or/and changing the private key did not require any changes in the encryption and decryption functions. The proposed method was tested and implemented using various images, the obtained results proved the quality, sensitivity and the performance of the method.

References

[1]. Ahmad, M., Alsharari, H. D., & Nizam, M. (2014). Security improvement of an image encryption based on mPixel-chaotic-shuffle and pixel-chaotic-diffusion. arXiv:1403.6626.

[2]. Thiyagarajan J, Murugan B, Gounden NGA. A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity. *Serbian Journal of Electrical Engineering.* 2019;16(2):247–265. doi: 10.2298/SJEE1902247T.

[3]. Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map. *Image and Vision Computing.* 2006;24(9):926–934. doi: 10.1016/j.imavis.2006.02.021.

[4]. Bhattacharjee S, Gupta M, Chatterjee B. Time Efficient Image Encryption-Decryption for Visible and COVID-19 X-ray Images Using Modified Chaos-Based Logistic Map. Appl Biochem Biotechnol. 2023 Apr;195(4):2395-2413. doi: 10.1007/s12010-022-04161-7. Epub 2022 Sep 24. PMID: 36152105; PMCID: PMC9510176.

[5]. Curiac DI, Volosencu C (2012) Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest. Mathematics Problem in Engineering, 1–18.

[6]. Wang X, Zhu X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics Lasers Eng 107:370–379.

[7]. Rehman AU, Liao X, Kulsoom A, Abbas SA (2015) Selective encryption for gray images based on chaos and DNA complementary rules. Multimed Tools Applic 74(13):4655–4677.

[8]. Guesmi R, Farah MAB, Kachouri A, Samet M (2016) A novel chaos based image encryption using DNA sequence operation and secure hash algorithm SHA-2. Nonlinear Dynam 83(3):1123–1136

[9]. Tahir Sajjad Ali, Rashid Ali, A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box, Multimedia Tools and Applications (2022) 81:20585–20609.

[10]. Naji, A.W., Hameed, S.A., Zaidan, B.B., Al-Khateeb, W.F., Khalifa, O.O., Zaidan, A.A., Gunawan, T.S. (2009). Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. International Journal of Computer Science and Information Security (IJCSIS), 3(1): 73-78. arXiv:0908.0216.

[11]. Hamdan, A., Jalab, H.A., Zaidan, A.A., Zaidan, B.B. (2010). New frame work of hidden data with in non multimedia file. Int. J. Comput. Netw. Secur, 2(1): 46-54.

[12]. Taqa, A., Zaidan, A.A., Zaidan, B.B. (2009). New framework for high secure data hidden in the MPEG using AES encryption algorithm. International Journal of Computer and Electrical Engineering, 1(5): 1793-8163.

[13]. Ignatiev, A., Morgado, A., Marques-Silva, J. (2019). RC2: An efficient MaxSAT solver. Journal on Satisfiability, Boolean Modeling and Computation, 11(1): 53-64.

[14]. Verma, P., Shekhar, J., Preety, A.A. (2015). A survey for performance analysis various cryptography techniques digital contents. International Journal of Computer Science and Mobile Computing, 4(1): 522-531. https://doi.org/10.3233/SAT19011.

[15]. Alanazi, H., Zaidan, B.B., Zaidan, A.A., Jalab, H.A., Shabbir, M., Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. Journal of Computing, 2(3). arXiv:1003.4085.

[16]. Thakur, J., Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. International Journal of Emerging Technology and Advanced Engineering, 1(2): 6-12.

[17]. Mua'ad M. Abu-Faraj, Khaled Aldebei, Ziad A. Alqadi, Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography, Traiteme du, vol. 39, issue 1, 2022.

[18]. Mua'ad M. Abu-Faraj, Khaled Aldebei2, Ziad A. Alqadi, Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography, Traitement du Signal, vol. 39, issue 1, pp. 173-178, 2022.

[19]. Alqadi, Z. (2019). A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE), 9(5): 4092-4098.https://doi.org/10.11591/ijece.v9i5.pp4092-4098.

[20]. Alqadi, Z. (2009). A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image. Journal of Computer Science, 5(5): 355-362.

[21]. Zaini, H., Alqadi, Z.A. (2021). Efficient WPT based speech signal protection. IJCSMC, 10(9): 53-65. https://doi.org/10.47760/ijcsmc.2021.v10i09.006.
[22]. Zneit, R.A., Khrisat, M.S., Khawatreh, S.A., Alqadi, Z. (2020). Two ways to improve WPT decomposition used for image features extraction. European Journal of Scientific Research, 157(2): 195-205.
[23]. Hindi, A., Qaryouti, G.M., Eltous, Y., Abuzalata, M., Alqadi Z. (2020). Color image compression using linear prediction coding. International Journal of Computer Science and Mobile Computing, 9(2): 13-2.
[24]. Prof. Qazem Jabber Prof. Ziad Alqadi, Digital Image Cryptography using Index Keys, International Journal of Computer Science and Mobile Computing, vol. 12, issue 2, pp. 26 – 37, 2023.
[25]. Hatim Zaini, Ziad Alqadi, Improving Average and Median Filters, International Journal of Computer Science and Mobile Computing, Vol. 12, Issue. 2, pg.1 – 13, 2023.
[26]. Hatim Zaini, Ziad Alqadi, Long Messages Segmentation for Efficient Message Cryptography, IJCSMC, vol. 12, issue 1, pp. 59-69, 2023.
[27]. Ziad A. Alqadi and Nasser Abdellati Adnan Manasreh, Mohammad S. Khrisat, Hatim Ghazi Zaini, IMPROVING DATA STANDARD METHODS OF CRYPTOGRAPHY, ARPN Journal of Engineering and Applied Sciences, vol. 17, issue 24, pp. 2077-2088, 2023.
[28]. Zaid Alqadi and Basel J. A. Ali Mua'ad Abu-Faraj, Abeer Al-Hyarib, Ismail Altaharwaa, Increasing the security of transmitted text messages using chaotic key and image key cryptography, International Journal of Data and Network Science, vol. 7, pp. 1-12, 2023.
[29]. Abdullah N Olimat, Ali F Al-Shawabkeh, Ziad A Al-Qadi, Nijad A Al-Najdawi, Ahmed Al-Salaymeh, Experimental study and computational approach prediction on thermal performance of eutectic salt inside a latent heat storage prototype, Thermal Science and Engineering Progress, Volume 37, 101606, 2023.
[30]. Mohammad S Khrisat, Ziad A Alqadi, Enhancing LSB Method Performance Using Secret Message Segmentation, IJCSNS, vol. 22, issue 7, pp. 1-6, 2022.
[31]. F. Omar and Z. A. Alqadi, M. M. Al-Laham, Digital Image Slicing to Strengthen the Security of LSB Technique of Encrypting Text Messages, 2022 International Arab Conference on Information Technology (ACIT), pp. 1-6, 2022.
[32]. Hatim Ghazi Zaini and Ziad A. Alqadi Adnan Manasreh, Mohammad S. Khrisat, COLOR IMAGES STEGANOGRAPHY BY IMPLEMENTING SIMPLE LOGICAL OPERATIONS USING ASELECTED STEGANOGRAPHIC FACTOR, ARPN Journal of Engineering and Applied Sciences, vol. 17, issue 17, pp. 1602-1610, 2022.
[33]. Aamer Nadeem, Dr M. Yuns Javed, A Performance Comparison of Data Encryption Algorithms, Conference Paper · September 2005 DOI: 10.1109/ICICT.2005.1598556 · Source: IEEE Explore.
[34]. Prof. Ziad Alqadi, Modified LSB2 Steganography Method to Secure the Embedded Secret Message, International Journal of Computer Science and Mobile Computing, vol. 11, issue 8, pp. 22 – 44, 2022.
[35]. Dr. Dojana, Prof. Ziad Alqadi, Digital Image Cryptography using Lookup Table, International Journal of Computer Science and Mobile Computing, vol. 11, issue 11, pp. 180 – 199, 2022.
[36]. Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2018.
[37]. Akram A. Moustafa and Ziad A. Alqadi, A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image, Journal of Computer Science 5 (5): 355-362, 2009.
[38]. ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.
[39]. Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.
[40]. Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.
[41]. Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952, 2010.
[42]. Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009. [20].A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using a New R'G'I Model", Journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.
[43]. K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014.
[44]. J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher, "A Novel zero-error method to create a secret tag for an image", Journal of Theoretical and Applied Information Technology, Vol. 96. No. 13, pp. 4081-4091, 2018.

[45]. Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.

[46]. M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014.

[47]. M. Juneja, P. S. Sandhu, An improved LSB based Steganography with enhanced Security and Embedding/Extraction, 3rd International Conference on Intelligent Computational Systems, Hong Kong China, January 26-27, 2013.

[48]. H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A alqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology (I.RE.I.T.) Vol. 1, N. 6 ISSN 2281-2911.

[49]. Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein A COMPARISON BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5, October 2016.

[50]. Z.A. Alqadi, A. Abu-Jazar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.

[51]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh: A Novel Based On Image Blocking Method to Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization, 2019.

[52]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology 15th July 2018.

[53]. Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.

[54]. Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata: Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications (0975 – 8887). Volume 153 – No2, November 2016.

[55]. Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 76-90.

[56]. Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103.

[57]. Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.

[58]. Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019.

[59]. Rashad J. Rasras, Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 14-26.

[60]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh; A Novel Based on Image Blocking Method to Encrypt-Decrypt Color; INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION VOL 3, (2019).

[61]. B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh, "A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 10, 2018.

[62]. J. AL-AZZEH, B. ZAHRAN, Z. ALQADI, B. AYYOUB, M. ABU-ZAHER, "A novel Zero-error Method to Create a Secret Tag for an Image", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 13, 2018.pp: 4081-4091.

[63]. J. AL-AZZEH, B. ZAHRAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.

[64]. Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.

[65]. Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.

[66]. Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences, vol. 48, issue 12, pp. 177-182, 2022.

[67]. Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.

[68]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022, doi.org/10.3390/sym14040664.

[69]. M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6, pp. 685-694, 2021, doi:10.35741/issn.0258-2724.56.6.61.

[70]. M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[71]. M. Abu-Faraj, and Z. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no. 12, pp. 648-656, 2021, doi: 10.22937/IJCSNS.2021.21.12.89.

[72]. M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61.

[73]. M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8.

